

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT (PCT Article 36 and Rule 70)



Applicant's or agent's file reference P016008WONAR		FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA416)	
International application No. PCT/GB 03/04256	International filing date (day/month/year) 06.10.2003	Priority date (day/month/year) 12.12.2002	
International Patent Classification (IPC) or both national classification and IPC G06F1/00			
Applicant ARM LIMITED			

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

 These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:
 - ☒ Basis of the opinion
 - ☐ Priority
 - ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - ☐ Lack of unity of invention
 - ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - ☐ Certain documents cited
 - ☐ Certain defects in the international application
 - ☐ Certain observations on the international application

Date of submission of the demand 15.06.2004	Date of completion of this report 24.01.2005
Name and mailing address of the international preliminary examining authority:  European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Authorized Officer Alecú, M Telephone No. +31 70 340-2648 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB 03/04256

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

4-14 as originally filed
1-3 received on 01.11.2004 with letter of 29.10.2004

Claims, Numbers

1-12 received on 05.01.2005 with letter of 04.01.2005

Drawings, Sheets

1/11-11/11 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/GB 03/04256**

5. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

see separate sheet

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	2,4,5,6,8,10-12
	No: Claims	1,3,7,9
Inventive step (IS)	Yes: Claims	2,5,8,11
	No: Claims	1,3,4,6,7,9,10,12
Industrial applicability (IA)	Yes: Claims	1-12
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item I

Basis of the report

The amendments filed with the letter dated 4 January 2005 introduce subject-matter which extends beyond the content of the application as filed, contrary to Article 34(2)(b) PCT.

Amended claim 1 claims an apparatus for processing data, said apparatus comprising:

....

- a. three or more further registers; wherein when said register write circuit writes a data value to said data processing register, said register write circuit also writes data values to
- b. three or more further registers such that a fixed relative number of bits within said data processing register and said
- c. three or more further registers as a whole ...

Original claim 1 was claiming an apparatus for processing data, said apparatus comprising:

...

- d. one or more further registers; wherein said register write circuit acts such that a fixed relative number of bits within said data processing register and said
- e. one or more further registers as a whole ...

The original claim (and the first page of the description where the same wording is present) provides support for the range of "one or more further registers". However, disclosing the use of "one or more further registers" is not the same as disclosing the use of one, two, three, four, five, six ... further registers.

In particular the use of four (or any other value greater than three) further registers is not explicitly disclosed, nor directly and unambiguously derivable from the application as filed. A preferred embodiment, presented on page 2 of the original description, teaches the use of only three further registers.

Figure 9 shows fourteen dedicated dummy registers and two shared dummy registers, so it provides support for the first use of "three or more further registers" (a.). However it is not directly and unambiguously derivable from Figure 9, nor from any other part of the application as originally filed that when the register write circuit writes a data value to the data processing register, said register write circuit also writes data values to three **or more** further registers. In the light of the description of Figure 9 and of the application as a whole, the skilled person could reasonably understand that, when writing to register R12 (as an example) also a write

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/04256

to three further registers (the dummy register corresponding to R12 and the two shared dummy registers) occurs. There is nothing to indicate that a write to more than these three registers is necessary.

Therefore an apparatus as claimed in amended claim 1 is not directly and unambiguously derivable from the original application.

Since the wording of claim 1 is the same also in the set of amendments filed with the letter dated 29 October 2004, also this set of amendments introduce subject-matter which extends beyond the content of the application as filed, contrary to Article 34(2)(b) PCT, for the same reasons previously mentioned.

The report will be established based on the original set of application documents.

Re Item V

**Reasoned statement with regard to novelty, inventive step or industrial applicability;
citations and explanations supporting such statement**

Reference is made to the following document:

D1: WO 99/67766 A (CRYPTOGRAPHY RESEARCH INC ; KOCHER PAUL C (US); JAFFE JOSHUA M (US); J) 29 December 1999 (1999-12-29)

1. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1 and 7 is not new in the sense of Article 33(2) PCT.

Document D1 discloses:

Apparatus for processing data (D1, page 23, line 9 -"tamper-resistant microprocessors"), said apparatus comprising:

a data processing register operable to store a data value (implicit in a microprocessor);
a register writing circuit operable to store a data value to said data processing register (implicit in a microprocessor); and
one or more further registers (at least one further register is implicit in a microprocessor);
wherein said register write circuit acts such that a fixed relative number of bits within said data processing register and said one or more further registers as a whole transition from high to

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/04256

low and from low to high irrespective of what data value is being written to data processing register and what data value is being written to data processing register and what value was previously stored within said data processing register (see D1, page 7, "Fixed Transition Count Computation")

2. Dependent claims 3,4,6,9,10,12 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty (Article 33 (2) PCT) or inventive step (Article 33(3) PCT) with regard to the documents cited in the search report and/or general knowledge of the skilled person.

3. Claim 1 claims an apparatus in which a register write circuit acts such that a fixed relative number of bits within data processing registers transition from high to low and from low to high.

This formulation is very broad and includes embodiments which are clearly not supported by the description: e.g. the claimed apparatus could be implemented such that the fixed relative number of bits transitions is intrinsically achieved by the technology which is used (see D1 for an example of such technology).

However the teaching of the description is that the register write circuit, based on the formula of page 2, lines 14 to 17, writes appropriate data values to three further registers at the same time (see page 1, line 32 - page 2, line 2).

Therefore claim 1 is not supported by the description (Article 6 PCT).

3.1 The case of only one further register, claimed in claim 1, is also not supported by the description, Article 6 PCT, because the description provides only examples using three further registers. It is not clear how this teaching can be extended to the case of less than 3 further registers.

If, for example, one further register is used to store the inverted value written in the data processing register, the number of ones and zeros in both registers as a whole will be constant, but the number of transitions will vary depending on the actual and previous data stored in the register.

3.2 The above objections apply also, mutatis mutandis, to claim 7.

3.3 The formula used in claim 5 for the shared dummy registers is different from the formula used in claim 2 (a XOR with the previous value of the shared register is missing). This leads

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/04256

to the fact that it is no longer clear which value is actually stored in these shared registers and therefore the matter for which protection is sought is not clear.

3.4 The above objection applies also, mutatis mutandis, to claim 11.

3.5 By reading the description it appears that the formula presented in claims 2 and 8 is the correct one and that a typing mistake was made in claims 5 and 11.

For the purpose of this written opinion it is considered that the formula presented in claims 5 and 11 is the same as the one presented in claim 2.

3.6 The combination of the features of dependent claims 2,5,8 and 11 is neither known from, nor rendered obvious by, the available prior art, since the additional technical features present in these claims is not disclosed, nor suggested in the available prior art.

CLAIMS

05.01.2005

(96)

1. Apparatus for processing data, said apparatus comprising:
a data processing register operable to store a data value;
5 a register writing circuit operable to store a data value to said data processing register; and
three or more further registers; wherein
when said register write circuit writes a data value to said data processing register, said register write circuit also writes data values to three or more further
10 registers such that a fixed relative number of bits within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what data value is being written to said data processing register and what data value was previously stored within said data processing register.
- 15 2. Apparatus as claimed in claim 1, wherein when said register write circuit writes a value X_i to an i^{th} bit of said data processing register previously storing a value of Y_i , said register write circuit also writes to corresponding bit positions within three further registers respective values of:
20 an inverse of X_i ;
a new value Rd_i given by $(\text{inverse}(X_i \text{ XOR } Y_i)) \text{ XOR } (\text{a value of } Rd_i \text{ currently stored});$ and
an inverse of said new value of Rd_i .
- 25 3. Apparatus as claimed in any one of claims 1 and 2, wherein said data processing register is one of a plurality of data processing registers of a register bank.
4. Apparatus as claimed in claim 2, wherein said three further registers comprise a dedicated dummy register dedicated to said data processing register and two shared
30 dummy registers shared between said plurality of data processing registers of said register bank.
5. Apparatus as claimed in claim 1, wherein when said register write circuit writes a value X_i to an i^{th} bit of said data processing register previously storing a value
35 of Y_i , said register write circuit also writes to corresponding bit positions within three

further registers comprising a dedicated dummy register dedicated to said data processing register and two shared dummy registers shared between said plurality of data processing registers of said register bank such that said dedicated dummy register stores said inverse of X_i and said two shared dummy registers store said exclusive logical OR of X_i with Y_i and said inverse of the exclusive logical OR of X_i with Y_i .

10

6. Apparatus as claimed in any one of claims 4 and 5, wherein said three further registers are provided for a subset of said plurality of data processing registers of said register bank.

15

7. A method of processing data, said method comprising the steps of:
storing a data value in a data processing register; and
when said data value is stored in said data processing register also storing data values within three or more further registers such than a fixed relative number of bits within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what said data value is being written to data processing register and what data value was previously stored within said data processing register.

20

8. A method as claimed in claim 7, wherein when writing a value X_i to an i^{th} bit of said data processing register previously storing a value of Y_i , also writing to corresponding bit positions within three further registers respective values of:
an inverse of X_i ;
a new value Rd_i given by $(\text{inverse}(X_i \text{ XOR } Y_i)) \text{ XOR } (\text{a value of } Rd_i \text{ currently stored})$; and
an inverse of said new value of Rd_i .

25

9. A method as claimed in any one of claims 7 and 8, wherein said data processing register is one of a plurality of data processing registers of a register bank.

30

10. A method as claimed in claim 8, wherein said three further registers comprise a dedicated dummy register dedicated to said data processing register and two shared dummy registers shared between said plurality of data processing registers of said register bank.

35

11. A method as claimed in claim 7, wherein when writing a value X_i to an i^{th} bit of said data processing register previously storing a value of Y_i , also writing to corresponding bit positions within three further registers comprising a dedicated dummy register dedicated to said data processing register and two shared dummy registers shared between said plurality of data processing registers of said register bank such that said dedicated dummy register stores said inverse of X_i and said two shared dummy registers store said exclusive logical OR of X_i with Y_i and said inverse of the exclusive logical OR of X_i with Y_i .
12. A method as claimed in any one of claims 10 and 11, wherein said three further registers are provided for a subset of said plurality of data processing registers of said register bank.

CLAIMS

01.11.2004

(78)

1. Apparatus for processing data, said apparatus comprising:
a data processing register operable to store a data value;
5 a register writing circuit operable to store a data value to said data processing register; and
three or more further registers; wherein
when said register write circuit writes a data value to said data processing register, said register write circuit also writes data values to three or more further
10 registers such that a fixed relative number of bits within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what data value is being written to said data processing register and what data value was previously stored within said data processing register.
- 15 2. Apparatus as claimed in claim 1, wherein when said register writing circuit writes a value X_i to an i^{th} bit of said data processing register previously storing a value of Y_i , said register writing circuit also writes to corresponding bit positions within three further registers respective values of:
20 an inverse of X_i ;
a new value Rd_i given by $(\text{inverse}(X_i \text{ XOR } Y_i)) \text{ XOR } (\text{a value of } Rd_i \text{ currently stored})$; and
an inverse of said new value of Rd_i .
- 25 3. Apparatus as claimed in any one of claims 1 and 2, wherein said data processing register is one of a plurality of data processing registers of a register bank.
4. Apparatus as claimed in claim 2, wherein said three further registers comprise a dedicated dummy register dedicated to said data processing register and two shared
30 dummy registers shared between said plurality of data processing registers of said register bank.
5. Apparatus as claimed in claim 4, wherein said dedicated dummy register stores said inverse of X_i and said two shared dummy registers store said exclusive
35 logical OR of X_i with Y_i and said inverse of the exclusive logical OR of X_i with Y_i .

6. Apparatus as claimed in any one of claims 4 and 5, wherein said three further registers are provided for a subset of said plurality of data processing registers of said register bank.

5

7. A method of processing data, said method comprising the steps of:
storing a data value in a data processing register; and
when said data value is stored in said data processing register also storing data values within three or more further registers such than a fixed relative number of bits within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what said data value is being written to data processing register and what data value was previously stored within said data processing register.

10

15

8. A method as claimed in claim 7, wherein when writing a value X_i to an i^{th} bit of said data processing register previously storing a value of Y_i , also writing to corresponding bit positions within three further registers respective values of:
an inverse of X_i ;
a new value Rd_i given by $(\text{inverse}(X_i \text{ XOR } Y_i)) \text{ XOR (a value of } Rd_i \text{ currently stored)}$); and
an inverse of said new value of Rd_i .

20

9. A method as claimed in any one of claims 7 and 8, wherein said data processing register is one of a plurality of data processing registers of a register bank.

25

10. A method as claimed in claim 8, wherein said three further registers comprise a dedicated dummy register dedicated to said data processing register and two shared dummy registers shared between said plurality of data processing registers of said register bank.

30

11. A method as claimed in claim 10, wherein said dedicated dummy register stores said inverse of X_i and said two shared dummy registers store said exclusive logical OR of X_i with Y_i and said inverse of the exclusive logical OR of X_i with Y_i .

12. A method as claimed in any one of claims 10 and 11, wherein said three further registers are provided for a subset of said plurality of data processing registers of said register bank.

PROCESSING ACTIVITY MASKING IN A
DATA PROCESSING SYSTEM

01.11.2004

(78)

5 This invention relates to the field of data processing systems. More particularly, this invention relates to the masking of processing activity within data processing systems, for example, in order to increase security.

10 It is known to provide data processing systems which manipulate secure data and for which it is desirable to ensure a high degree of security. As an example, it is known to provide smart cards which include a data processing system which manipulates secure data, such as secret cryptographic keys, and this data must be kept secret in order to prevent fraud.

15 Known ways of attacking the security of such systems include timing analysis and power analysis. By observing the timing behaviour and/or the power consumption behaviour of such a system in response to inputs, information concerning the processing being performed and the data being manipulated can be determined in a way that can compromise security. It is strongly advantageous to provide resistance against such security attacks.

Viewed from one aspect the present invention provides apparatus for processing data, said apparatus comprising:

20 a data processing register operable to store a data value;
a register writing circuit operable to store a data value to said data processing register; and
three or more further registers; wherein
when said register write circuit writes a data value to said data processing register,
25 said register write circuit also writes data values to three or more further registers such that a fixed relative number of bits within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what data value is being written to said data processing register and what data value was previously stored within said data processing register.

30 This invention recognises that when a register write occurs there can be a difference in the power consumed and/or other characteristics depending upon how many bit values transition from high to low compared with how many bit values transition from low to high. The invention overcomes this problem by providing three or more further registers to which appropriate data values are written at the same time.
35 such that the number of high to low transitions and low to high transitions does not

change irrespective of what data value is being written and what the previous data value was. This enhances security by masking potentially externally visible characteristics having a dependence upon data values being processed. The technique is also applicable to systems in which multiple writes occur in parallel to multiple registers, e.g. a superscalar processor.

Whilst it is possible that a variety of different mathematical relationships may be determined between the true data value being written and the data values written in the three or more further registers that will satisfy the non - varying requirement, particularly preferred embodiments of the invention which are advantageously simple are such that said register writing circuit writes a value X_i to an i^{th} bit of said data processing register previously storing a value of Y_i , said register writing circuit also writes to corresponding bit positions within three further registers respective values of:

an inverse of X_i ;

a new value Rd_i given by $(\text{inverse}(X_i \text{ XOR } Y_i)) \text{ XOR } (\text{a value of } Rd_i \text{ currently stored})$; and

an inverse said new value of Rd_i .

This particular relationship balances the transitions and yet is relatively simple to calculate and uses relatively few further registers in a manner which is advantageous from a circuit requirement and power consumption point of view.

Whilst the present invention could be used to protect against the leakage of information due to writes from a single data register, the invention is well suited to embodiments in which a register bank of a plurality of data registers is provided.

Within such an environment dedicated dummy registers may be provided in combination with some shared dummy registers. The sharing of some of the dummy registers enables the circuit resources needed for this techniques to be advantageously reduced whilst still allowing a guaranteed balance in the number of transitions from high to low and low to high.

It is convenient to provide embodiments to which the dedicated dummy register stores the inverse of the value held within the real data register and the shared dummy registers store the exclusive OR of the new data value with the old data value as well as the inverse of this exclusive OR.

Whilst this technique may be utilised for all of the registers within a register bank, it is often the case that some registers within the register bank have dedicated

non-secure roles, such as program counter, stack pointer, return address and the like, which mean that the balance between the additional circuit resources required against the security issue is such that it is preferred not to utilise this technique in association with those registers.

5 Viewed from another aspect the present invention provides a method of processing data, said method comprising the steps of:

storing a data value in a data processing register; and

when said data value is stored in said data processing register also storing data values within three or more further registers such than a fixed relative number of bits
10 within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what said data value is being written to data processing register and what data value was previously stored within said data processing register.

Embodiments of the invention will now be described, by way of example only,
15 with reference to the accompanying drawings in which:

Figure 1 schematically illustrates a data processing system operable in a fixed timing mode and a variable timing mode;

Figure 2 schematically illustrates a conditional programming instruction;

Figure 3 is a flow diagram schematically illustrating part of the processing
20 operations performed by an instruction decoder operating in accordance with the present techniques;

Figure 4 schematically illustrates the execution of a conditional branch instruction in a fixed timing mode;

Figure 5 is a diagram schematically illustrating a data processing system
25 including multiple circuit portions which may be selectively enabled to perform required processing operations or dummy processing operations;

Figure 6 schematically illustrates a circuit portion and its associated dummy activity enabling circuit which may be responsive to both required enable signals and random dummy activity enable signals;

30 Figure 7 schematically illustrates a linear shift back feed register which may be used as a pseudo-random signal generator:

Figure 8 is a flow diagram schematically illustrating control of a circuit portion to perform required processing activity and dummy processing activity;

Figure 9 schematically illustrates a portion of a register bank including
35 multiple data processing registers, multiple dummy registers, multiple shared dummy